International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1333

(01/2022)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Secure applications and services (2) – Smart grid security

Security guidelines for the use of remote access tools in Internet-connected control systems

Recommendation ITU-T X.1333

ITU-T X-SERIES RECOMMENDATIONS

DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	X.1–X.199
OPEN SYSTEMS INTERCONNECTION	X.200–X.299
INTERWORKING BETWEEN NETWORKS	X.300–X.399
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600–X.699
OSI MANAGEMENT	X.700–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	X.850–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
INFORMATION AND NETWORK SECURITY	
General security aspects	X.1000–X.1029
Network security	X.1030–X.1049
Security management	X.1050–X.1069
Telebiometrics	X.1080–X.1099
SECURE APPLICATIONS AND SERVICES (1)	
Multicast security	X.1100–X.1109
Home network security	X.1110–X.1119
Mobile security	X.1120–X.1139
Web security (1)	X.1140–X.1149
Application Security (1)	X.1150–X.1159
Peer-to-peer security	X.1160–X.1169
Networked ID security	X.1170–X.1179
IPTV security	X.1180–X.1199
CYBERSPACE SECURITY	
Cybersecurity	X.1200–X.1229
Countering spam	X.1230–X.1249
Identity management	X.1250–X.1279
SECURE APPLICATIONS AND SERVICES (2)	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1319
Smart grid security	**X.1330–X.1339**
Certified mail	X.1340–X.1349
Internet of things (IoT) security	X.1350–X.1369
Intelligent transportation system (ITS) security	X.1370–X.1399
Distributed ledger technology (DLT) security	X.1400–X.1429
Application Security (2)	X.1450–X.1459
Web security (2)	X.1470–X.1489
CYBERSECURITY INFORMATION EXCHANGE	
Overview of cybersecurity	X.1500–X.1519
Vulnerability/state exchange	X.1520–X.1539
Event/incident/heuristics exchange	X.1540–X.1549
Exchange of policies	X.1550–X.1559
Heuristics and information request	X.1560–X.1569
Identification and discovery	X.1570–X.1579
Assured exchange	X.1580–X.1589
Cyber Defence	X.1590–X.1599
CLOUD COMPUTING SECURITY	
Overview of cloud computing security	X.1600–X.1601
Cloud computing security design	X.1602–X.1639
Cloud computing security best practices and guidelines	X.1640–X.1659
Cloud computing security implementation	X.1660–X.1679
Other cloud computing security	X.1680–X.1699
QUANTUM COMMUNICATION	
Terminologies	X.1700–X.1701
Quantum random number generator	X.1702–X.1709
Framework of QKDN security	X.1710–X.1711
Security design for QKDN	X.1712–X.1719
Security techniques for QKDN	X.1720–X.1729
DATA SECURITY	
Big Data Security	X.1750–X.1759
Data protection	X.1770–X.1789
IMT-2020 SECURITY	X.1800–X.1819

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T X.1333

Security guidelines for the use of remote access tools in Internet-connected control systems

Summary

Remote access tools (RATs) are widely used on control systems for monitoring, control and maintenance to reduce maintenance costs and minimize the response time in the event of a malfunction. RATs provide the ability to manipulate control systems remotely, but at the same time, an insecure configuration of RATs and vulnerabilities in RATs could significantly increase the attack surface of control systems. The most serious problem is an interface to access a control system from the external networks that could allow attackers access to the control system from the Internet.

Recommendation ITU-T X.1333 describes an overall picture to employ RATs securely for monitoring, control and maintenance. In this Recommendation, threats to network configuration due to the use of RATs are identified and security guidelines are provided to adapt secure configuration and security measures for the use of RATs in Internet-connected control systems.

Providing well-organized security controls on the use of RATs would be helpful for digital service providers operating control systems to reduce the attack surface and the threats from external networks. Moreover, it would be beneficial to align the security levels between developed and developing countries, since this is not a local problem, but a global problem.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1333	2022-01-07	17	11.1002/1000/14798

Keywords

Control system, guideline, remote access tool, security.

---

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents/software copyrights, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the appropriate ITU-T databases available via the ITU-T website at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Recommendation ITU-T X1333

Security guidelines for the use of remote access tools in Internet-connected control systems

1 Scope

This Recommendation provides security guidelines for the use of remote access tools (RATs) in Internet-connected control systems over telecommunication networks. It covers the following:

- Identification of threats against the insecure configuration of RATs and their impact on Internet-connected control systems;
- Security controls and their rationale for secure configuration of RATs;
- Implementation guidelines for each security control; and
- An example of a secure configuration of RAT in Appendix I.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

None.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following term defined elsewhere:

3.1.1 human machine interface (HMI) [b-IEC 61924-2]: The part of a system an operator interacts with. The interface is the aggregate of means by which the users interact with a machine, device, and system. The interface provides means for input, allowing the users to control the system and output, allowing the system to inform the users.

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

DDoS Distributed Denial of Service

DMZ Demilitarized Zone

DNS Domain Name Service

DoS Denial of Service

EWS Engineering Workstation

HMI Human Machine Interface

ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IPsec	Internet Protocol Security
LAN	Local Area Network
MAC	Media Access Control
MDM	Mobile Device Management
MDMS	Meter Data Management System
NAC	Network Access Control
NFC	Near Field Communication
PIN	Personal Identification Number
PLC	Programmable Logic Controller
RAT	Remote Access Tool
RFID	Radio Frequency Identification
SIEM	Security Information and Event Management
SSH	Secure Shell
SSL	Secure Socket Layer
TLS	Transport Layer Security
URL	Uniform Resource Locator
VM	Virtual Machine
VPN	Virtual Private Network

5 Conventions

This Recommendation uses the following conventions:

The keywords "should" indicate a requirement which is recommended but which is not absolutely required.

The keyword "may" indicate an optional requirement which is permissible, without implying any sense of being recommended.

In the body of this Recommendation, the word "can" or "could" sometimes appear, in which case they are to be interpreted as "is able to" or "was able to".

The appearance of the words "must", "should", "will" in Appendix I is to be interpreted as having no normative intent.

6 Overview – RATs in Internet-connected control systems

Control systems are employed to achieve an industrial objective such as manufacturing and transportation of matter or energy. The control system is responsible for ensuring the desired outcome or performance of the industrial objective. To ensure the performance of the control system, operators monitor information and data from sensors in field networks (see Figure 1). Based on the data and the information, operators may control the system if needed. To maintain the control system or solve technical problems, maintenance engineers from a control system vendor may access the control system.

Remote access tools (RATs) are widely used on industrial networks for control system monitoring, control and maintenance to reduce maintenance costs and minimize the response time in the event of a malfunction. According to a report [b-Kruglov et al.], in the first half of 2018, RATs were employed on 31.6% of control system computers, and this number did not include the number of remote desktop connections.

In most cases of control systems, RATs are commonly used to:

- monitor/control a human-machine interface (HMI) from an operator workstation;
- monitor/control a HMI from an engineering workstation;
- connect multiple operators to a single operator workstation;
- connect remote operators to an operator workstation via an external network; and
- provide maintenance of an Internet-connected control system from a computer of a maintenance engineer in a control system vendor via an external network.

These use cases show that the use of RATs for control system monitoring, control and maintenance could be indispensable requirements to operate control systems. Moreover, using RATs would reduce the maintenance costs. For example, in the first 3 bullets among use cases mentioned above, the number of licenses for the HMI software could be reduced. In addition, recent smart devices could also be used as RAT clients. End customers can monitor and control their photovoltaics (PVs), for instance, by using a RAT in their smartphone.

Figure 1 shows a general configuration for using RATs in Internet-connected control systems based on the use cases.

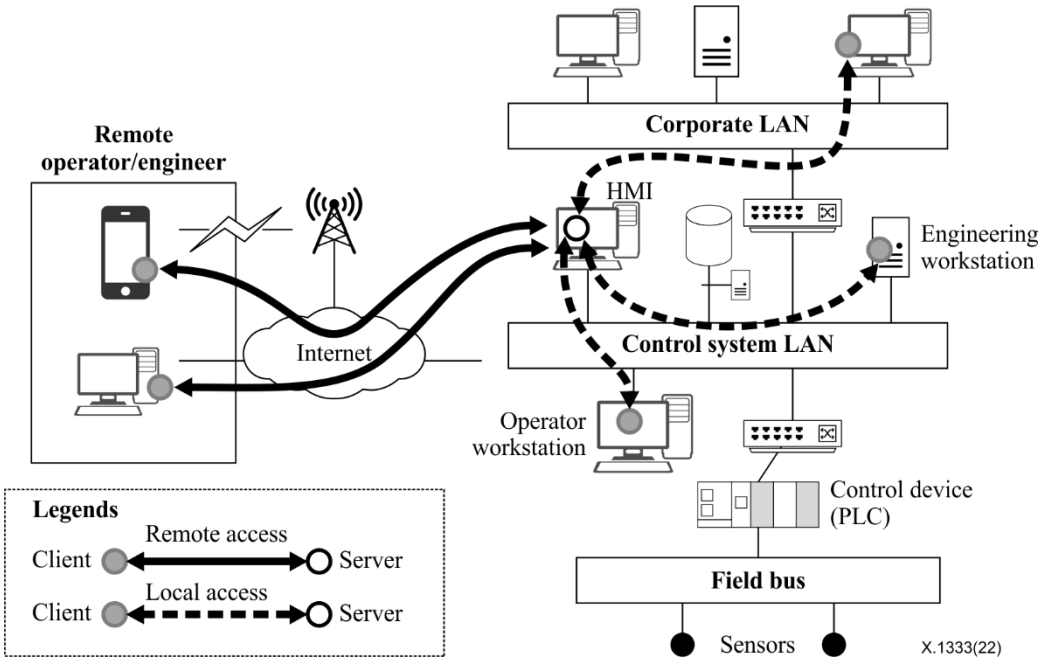

Figure 1 – Network configuration for using RATs in Internet-connected control systems

In other cases, an organization operating a control system could attach a small-sized control system to legacy control systems. A site running a bulk power generator, for example, could employ a new fuel cell system to increase its capacity with clean energy. Fuel cell systems include HMI computers, control devices, sensors, batteries and other systems. Thus, in this example, a HMI and control devices could be connected to the same subnetwork located in the field-side of the fuel cell system. Figure 2 shows the configuration for using RATs to access a HMI in the field.

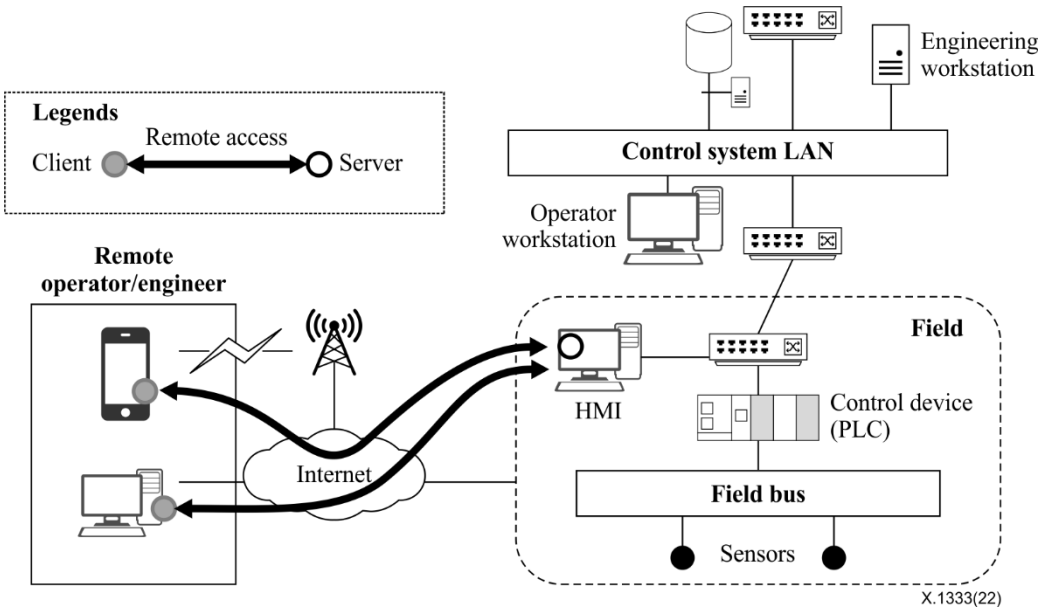

Figure 2 – Network configuration for using RATs in a field network of Internet-connected control systems

RATs provide the ability to manipulate control systems remotely and it help to reduce maintenance costs. However at the same time, an insecure configuration of RATs and vulnerabilities in RATs could significantly increase the attack surface of control systems. The most severe problem is that a RAT can be used as an interface for accessing an Internet-connected control system from the external networks, which can usually access from the Internet. Thus, once adversaries could compromise a RAT client for an Internet-connected control system, they could cause the malfunctioning of the system. Moreover, it is hard to detect their activities. Thus, this Recommendation focuses on RAT connections from the outside of Internet-connected control systems.

7 Threats to the use of RATs in Internet-connected control systems

7.1 Threats to RAT clients

A RAT client could be installed on a client computer in a remote place or a mobile device owned by a remote operator or a remote maintenance engineer. The remote location could be outside the physical protection of the organization and the logical protection of the organization's firewall. In addition, client computers could not be managed well while the organization's computers are closely managed and tightly locked down. Thus, a number of threats to the use of RATs could come from computers on which RAT client is installed.

The following threats to client computers and RAT clients should be considered:

- (T1) An attacker could exploit vulnerabilities in client computers or RAT clients to compromise client computers or RAT clients. Once attackers gain full control of the client computer or the RAT client, they could connect to the control system via the RAT.
- (T2) An adversary could exploit split tunneling in a client computer. Client computers are usually connected to not only RAT servers but also any other Internet-connected systems. Thus, an adversary who gets full control of the client computer can transmit critical information acquired from the control system via an unprotected Internet connection.
- (T3) An attacker could install targeted malware on a client computer, identify sensitive information (e.g., login ID and password), and exfiltrate the information. Once attackers

gain the information, they can access the RAT server by using a RAT client installed on any other machine rather than the client computer.

- (T4) An attacker could conduct a brute force attack, dictionary attack, or password cracking supported using open-source tools to gain access to a RAT server.
- (T5) Adversaries could conceal their activities on client computers by deleting log data. Due to this threat, an organization operating a control system may fail to track the adversary's activities when the organization investigates the incident.
- (T6) An adversary could exploit physical access to client computers.

7.2 Threats to RAT servers

A RAT server could be installed on an HMI machine in an Internet-connected control system. Since the server should open a service connected to the Internet, an adversary could exploit the port for the service. If the service is not be protected securely, the attacker could access to control system via the service.

The following threats to client computers and RAT clients should be considered:

- (T7) An attacker could exploit vulnerabilities in a RAT server or a machine on which the RAT server is installed to compromise the machine or RAT server. This kind of attack could lead to the attacker gaining full control of the control system. For instance, once attackers access the machine or the RAT server, they could elevate their rights in the device or acquire full control of the RAT server.
- (T8) An adversary could conduct distributed denial of service (DDoS) and denial of service (DoS) attacks against the RAT sever.

7.3 Threats to the communication channel between client and servers

Since the RAT server and client are connected via the Internet in an Internet-connected control system, the communication channel can be accessed by others. If communications are either unencrypted or encrypted with weak methods containing publicly known vulnerabilities, an adversary could take advantage of them and gain access to transferred information and channels.

The following threats to client computers and RAT clients should be considered:

- (T9) An adversary could take advantage of unprotected communication, gain sensitive information (e.g., login ID and password), and use the information to access to the RAT server. When a communication channel is protected by weak cryptography, an adversary could obtain the same result. Once adversaries manage to access the RAT server, they could take full control of the control system.
- (T10) An attacker could take advantage of a weak protocol containing publicly known vulnerabilities and gain access to the RAT server or cause a denial of service for users of the RAT servers.

8 Security guidelines for the use of RATs in Internet-connected control systems

8.1 Security guidelines for RAT clients

8.1.1 Software update

Security control

The RAT software, operating system and any other software on the client-side should be kept up-to-date.

Purpose

The software could have unknown vulnerabilities as attack techniques have been advanced. When a new vulnerability is announced, it is a 0-day vulnerability. Attackers could exploit the 0-day vulnerability to compromise the RAT client device. The number of vulnerabilities related to RAT software has increased recently. In 2019, 31 vulnerabilities for virtual network computing or VNC-like software have been discovered. RAT software vendors will provide a security patch when a new vulnerability has been released, users are able to mitigate the vulnerability by adopting the security patch. Keeping the software up-to-date is one of the easiest ways to keep client devices secure.

Implementation guidelines

To keep software up-to-date the most essential action is to regularly check if there is a new update. Unfortunately, it is not easy to make this regular check by users, thus the following automatic approach should be considered to keep software up-to-date.

a) A security update check method should be triggered whenever RAT client software is executed.

b) If there is a new version of the software or a new security update, it should be applied to the client software before executing it.

c) Security update check method may also be triggered regularly while the RAT client is running.

d) If there is a new version of the software or a new security update, it should be applied to the client software when it is terminated.

In some cases, the RAT client device should be restarted after installing a security patch. Unlike a typical client computer, the RAT client for the control system could not restart at that moment as the remote operator/engineer should monitor the control system continuously. In this environment, the security update check method installs the updates after acquiring the user's confirmation.

Additionally, the operating system and any other software in the device running RAT client software should also be updated. Automatic update capability of operating systems should be enabled. The security update for each application should be checked regularly and security patches applied promptly when the patches are available.

8.1.2 Software integrity

Security control

The integrity of RAT software on the client side should be protected.

Purpose

A modified version of RAT software could be installed on the client-side. An attacker could compromise the update server, or an attacker could distribute abnormal updates by a phishing email. The RAT software infected with malicious code behaves normally, but the malicious code works to leak information or establish a connection with an attacker when necessary. Thus, to prevent the misbehaviour of malicious RAT software, the integrity of RAT software should be protected.

Implementation guidelines

Since, as mentioned above, attackers are able to distribute the malicious RAT software via an official supply chain, it is problematic that the user must identify whether the software is modified or not. Thus, the automatic integrity check procedure should be employed to protect the integrity of RAT software.

For the automatic integrity check procedure, the following approach should be considered:

a) Integrity checking procedure should be initiated when the software is executed, or the update procedure is started.

b) The software or the update procedure should be started if there is no clue that the software is changed.

c) The status of the integrity checking procedure should be shown on the screen so that the user knows this software is normal.

d) Integrity value for software should be generated by a cryptographic method to ensure that the software is not modified by anyone else. For this method, a secure cryptographic algorithm should be used.

8.1.3 Secure configuration of RAT client

Security control

Configuration for RAT client-side should conform to the security policy of the organization owning the Internet-connected control system.

Purpose

Even though RAT software provides security capabilities for secure communication, RAT can only be used securely when it is properly configured. In general, users want to avoid inconvenience, so they do not want to enable security features and use a strong password. Moreover, regarding Internet protocol security (IPsec), where the user does not know the correct configuration details, these misconfigurations will increase the possibility of abusing the RAT client software.

Implementation guidelines

To reduce the possibility of RAT client's misconfiguration, it is better to configure the client by an organization that operates a control system. To manage the configuration of RAT clients by the organization, the following approaches should be considered:

a) Using static Internet protocol (IP) for RAT server: If a uniform resource locator URL is used for accessing to a virtual private network (VPN) gateway or RAT server, remote operators/engineers may be exposed to several attacks such as phishing, domain name service (DNS) spoofing and DNS cache poisoning. Using a static IP address or hard-coded IP address for the server-side makes it possible to mitigate those threats and provide server authentication for remote operators/engineers during the secure communication channel.

b) Network access control (NAC) solution or mobile device management (MDM): NAC provides capabilities to verify the status of a computer or laptop, while MDM supports capabilities to check and control mobile devices. NAC is helpful for organizations to induce remote operators/engineers to configure a computer running a RAT client by verifying the device's configurations before making a connection. If a device is misconfigured, NAC will ban network traffic from the device until remote operators/engineers fix the misconfiguration. If remote operators use mobile devices to access a RAT server, MDM is a substitute for NAC.

c) Virtual machine (VM) image: Organization owning a control system may distribute a VM image to remote operators/engineers. When the organization creates the image, all configurations related to the client device, VPN client and RAT client should be configured based on the organization's security policy. Moreover, to protect the VM image itself, it should be encrypted and should be stored on remote operators'/engineers' devices when it is not in use.

8.1.4 Control of user access to client device

Security control

Only authorized users should be allowed to access the RAT client software.

Purpose

If access to RAT client software is limited to authorized remote operators/engineers, the possibility of abusing the RAT client can be reduced.

However, legitimate remote operators/engineers can leave the place temporarily while they are using RAT software, and then there is a possibility of abusing the connected session. Thus, when remote operators/engineers stop or pause their work, the device should be locked. When remote operators/engineers return in front of the RAT client device, the operators/engineers are able to resume their work by using the established identification and authentication procedure.

Implementation guidelines

It is possible to implement this control by having remote operators/engineers use an account different from the account used to perform regular tasks when executing the RAT client software. In other words, a remote operator/engineer should have another account for using the RAT client. In addition, the password for the account should be strong.

Session locking is an efficient way to solve the latter issue. There are two types of session locking; 1) operating system-level session locking and 2) application-level session locking. Most operating systems have session locking capability, so it should be initiated after a period of inactivity. It depends on the RAT software, it is differs depending on whether application-level session locking capability is provided or not. Thus, the presence of session locking capability should be a major criterion when the organization operating control system chooses RAT software.

8.1.5 Physical security

Security requirement

Only authorized remote operators/engineers should be allowed to access the device running RAT client software physically, and the place where the operators/engineers use the devices should be protected from unauthorized access.

Purpose

Even though a device and RAT client software are securely configured to employ their security feature properly, the device and the place where the device is located should be protected from unauthorized access by any adversaries.

Implementation guidelines

For ensuring the physical security for devices, software and the environment using them, the following should be considered:

a) The office where remote operators/engineers work should be protected by a proper door access control system using near field communication (NFC) or radio frequency identification (RFID) technology. For stronger security, a biometric (e.g., fingerprint, iris, and face recognition) access control system may be considered.

b) A closed-circuit television camera should be installed in front of the door of the office.

c) A device running RAT client software should be protected from theft by using a cable lock or other deterrents.

8.2 Security guidelines for RAT servers

8.2.1 User authentication

Security control

A RAT service should allow users to remote access resources only when using two-factor authentication.

Purpose

Traditional ID and password authentication could be broken, and knowledge factors, such as a password or personal identification number (PIN), alone will not ensure that the accessing user is the person who has the appropriate permissions.

For local access, physical access control methods identify and allow legitimate users to access system resources. Accordingly, even if an attacker knows the ID and password of a legitimate user, it is not easy to access system resources directly. However, for remote access, it is not easy to apply physical security methods and user identification methods. Therefore, instead of the physical security methods, two-factor authentication could decrease the possibility of impersonation even if the ID and password have been stolen.

Implementation guidelines

The authentication factors may include something you know (knowledge factor), something you have (possession factor), something you are (inherent factor), and somewhere you are (location-based factor). Two-factor authentication currently tends to be implemented through possession factor and knowledge factor or inherent factor and knowledge factor.

Recently, most mobile devices (e.g., laptops, tablets, and smartphones) have biometric methods, thus inherent factors, including fingerprint, iris, or face, could likely be the best option for two-factor authentication.

In some circumstances, however, biometric methods are not possible to use. For example, if remote users have to wear gloves during their working hours, the fingerprint should be avoided. In these cases, possession factors such as cryptographic tokens could be applied.

Most RAT software provides the capability of limiting authentication waiting time. In that case, the RAT server will discard the authentication request if it does not receive a response from the user for a certain amount of time. Thus, it will be helpful to reduce the likelihood of a denial of service attacks.

8.2.2 User authorization

Security control

Accounts for remote users should have only the bare minimum privileges necessary to perform their function.

Purpose

To limit the impact of an attack, remote user's privileges should be limited to minimum privileges necessary to perform its function.

Implementation guidelines

RAT software, usually, does not provide a fine-grained authorization method. Most of RAT software provides only two sorts of modes such as read-only mode and fully-control mode. Thus, if attackers could access a RAT server, they could fully compromise the device. To avoid the threat, privileges granting to remote user's accounts should be limited to minimum privileges necessary to perform their functions.

For this, first of all, a remote user account should not be an administrator account, and no privilege, which is able to change the RAT server, should be granted to the remote user's account. Installing software, configuring OS, configuring the system may be one of the limited privileges.

Second, access control for an application should also be applied. The remote user account cannot run any other software except for the software operating and monitoring control system. If a remote user can open a terminal program on the RAT server's machine, the user may access another system via the RAT server. That would be an excellent benefit for attackers.

8.2.3 Periodic re-authentication

Security control

A RAT server should re-authenticate users and client devices after a period of time.

Purpose

To ensure that only authorized remote operators/engineers use remote access, a RAT server should require them to re-authenticate periodically during long remote access sessions. This helps to ensure that unauthorized persons could not use the remote access even if the device is stolen while a connection between the RAT server and the client has been established.

In addition, network-level re-authentication helps to reduce the likelihood of being exposed to session hijacking attacks.

Implementation guidelines

RAT server software itself does not provide the capability of re-authentication after a period of time, while most VPN gateways provide the security feature. Thus, to implement this control properly, VPN should be employed between the RAT client and server.

In addition, most VPN gateways provide the capability of client re-authentication. Therefore, the organization should enable the capability of a VPN gateway to authenticate a user or device after a period of time. For example, when RAT communication is carried over transport layer security (TLS) version 1.3, the post-handshake client authentication extension should be enabled. If the extension is enabled, a TLS server will request client authentication after establishing a TLS connection.

8.2.4 Software update

Security control

RAT server software, operating system and any other software in a server device should be kept up-to-date.

Purpose

The purposes corresponding to the control in clause 8.2.4 are the same as those specified in clause 8.1.1.

Implementation guidelines

The guidelines corresponding to the control in clause 8.2.4 are the same as those specified in clause 8.1.1.

8.3 Security guidelines for networks

8.3.1 Network access control

Security control

Only legitimate users should be allowed to access network communications between RAT server and RAT client.

Purpose

Accessing network communication is one of the first steps to compromise a service or a system. Attackers could gather information and data between a RAT server and client and inject falsified data to the communication channel, which could lead to a man-in-the-middle attack, malware distribution, and DoS attack. To protect the RAT service and control system, malicious users should be restricted from accessing network communications between RAT server and client.

Implementation guidelines

There are several ways to control access to network communication and protect their content. The following methods may be considered as options:

- A leased line may be employed to prevent unauthorized users from accessing the connection between the meter data management system (MDMS) and third-party service providers.
- Secure communication methods such as IPsec and secure socket layer (SSL) VPN should be applied to the communication between RAT client and server. RAT traffic should be tunneled within a VPN.
- If VPN is not feasible, remote access should be performed over TLS version 1.3 at least.

A secure cryptographic algorithm should be considered when a secure communication method, including VPN and TLS, is employed. [b-ITU-T X.1197] provides a list of examples of safe algorithms and key lengths. During communication channel setup, a VPN gateway or RAT server should reject a connection request if a client does not use a secure algorithm and key length.

8.3.2 Network level mutual authentication

Security control

Mutual authentication should be applied to the communication channel between RAT server and RAT client.

Purpose

A mutual authentication method for communication channels should be implemented so that a RAT client can verify the legitimacy of a RAT server before providing an authentication credential to it. With this function, the RAT service can avoid a man-in-the-middle attacks between the RAT client and server.

Implementation guidelines

When IPsec, SSL VPN or communication over TLS is employed in RAT communication, both a server's certificate and client's certificate should be used to authenticate each other. A client authenticates a server by verifying the server's certificate to ensure that the server is legitimate.

Most VPN solutions provide a server authentication feature, but this feature is not enabled in many cases. Thus, when a control system employs a VPN for protecting a RAT service, the server authentication option should be enabled.

Additionally, in TLS, usually only a server authenticates a client by verifying the client's credential, such as a certificate, because server authentication is an option. Thus, if a communication between a

server and a client is protected by the TLS for RAT service, exchanging each other's certificates between server and client should be required.

Lastly, the capability of authentication time out and the capability of limiting concurrent sessions should be enabled. Discarding connection requests properly, which are waiting for the client's authentication response, is a keystone for mitigating denial of service attacks.

8.3.3 Network misbehaviour detection

Security control

Network misbehaviour detection should be applied to the network to which a RAT server is connected.

Purpose

Even though various security methods are applied to RAT client-side, there is still a chance that the device running RAT client will be compromised. For example, if attackers can access the network of an Internet-connected control system via a compromised RAT client, they can also access any resources that are allowed to the RAT server. In that situation, the only difference between remote operators/engineers and attackers is behaviour. Remote operators/engineers know the network and the system they connected to, while attackers should need reconnaissance to figure out where the target is in the network. Accordingly, a network misbehaviour detection system based on network traffic could help to detect cyber-attacks.

Implementation guidelines

A network misbehaviour detection system should monitor and examine all messages between a RAT client and RAT server. Additionally, all messages from the device running a RAT server to any other devices in an Internet-connected control system should also be monitored and examined by the detection system. Thus, the detection system should be placed in the same sub-network where the RAT server is located, and it should collect traffic from the network device in which the port mirroring policy is enabled. For example, in a network like that shown in Figure 2, the port mirroring policy of the network switch in the field network is enabled, and the detection system collects traffic from the interface where the port mirroring policy is enabled.

When a secure communication method, such as IPsec, SSL VPN, or communication over TLS, is applied, the security device providing a secure communication channel should be placed at the sub-network perimeter where the RAT server is located. For instance, a VPN device should be placed before the network device so that the network misbehaviour detection system can check all packets.

The detection method can be classified into three types as static detection, misuse detection and anomaly detection. For the environment operating remote access tools, a combination of misuse detection and anomaly detection should be adopted to detect known attacks and unknown attacks.

8.3.4 Secure network configuration

Security control

A network where a RAT server is installed should be properly segmented and segregated.

Purpose

Network segmentation is the dividing of a network into several smaller networks, while network segregation is the enforcement of the policy to control the communication between hosts. By separating the network where the RAT server is installed from other networks, it is possible to prevent an attacker from accessing other control system resources even if the RAT server is breached.

Implementation guidelines

A network where a RAT server is installed should be separated from other networks in a control system, and communication from/to the RAT server should be controlled according to whitelist rules. It is possible to implement this type of security measure using the concept of a demilitarized zone (DMZ). A firewall partitions a sub-network containing the RAT server, and only authorized communication, such as 1) between RAT client and RAT server; 2) RAT server and other resources in a control system, is allowed based on the rules in the firewall. A service-level access control list may be applied for the firewall's rule. This means that the rules should be defined as a combination of IP address and port number.

For example, the HMI in the field network could be separated from the other resources in the field network by a firewall as shown in Figure 3. The firewall checks all packets from/to the RAT server according to its rules, and the rules are defined as which services on the RAT server are allowed to communicate with which services on other devices. Communication initiated by a service of engineering workstation (EWS) software on the HMI is allowed to arrive at the control device (i.e., the programmable logic controller (PLC) in Figure 3). In contrast, communication initiated by the secure shell (SSH) on the HMI is blocked by the firewall.

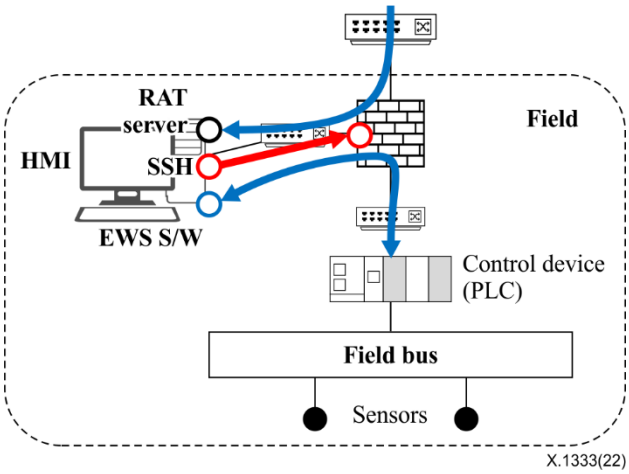

Figure 3 – Network segmentation and segregation for using RAT in a field network

8.4 Security guidelines for audit trails

8.4.1 Logging

Security control

System and network security events should be logged and the logs should be protected.

Purpose

System and network security event logs are the heart of the security management of any system. By reviewing and analysing the security-related events, security issues could be detected in time. Thus, the more granular event logs are generated by the RAT server, the more easily the organization detects security issues.

Implementation guidelines

Some RAT software provides the capability of more granular logging such as usage of each application and manipulation of data in the server device, while others supply the capability of simple logs such as connection to and disconnection from the RAT server. Thus, an organization should consider the granularity of security event logs generated by RAT software when they choose RAT software.

If the RAT software provides simple log capability, the organization should also consider the logging capability of the operating system where the RAT server is installed. For this, remote user accounts in the server device should be separated from other accounts. In this case, a security administrator should review security events recorded by the remote user account to detect misbehaviour.

In addition to the system event log, a network event log should also be generated. All RAT connection requests and their results (i.e., success or fail) should be logged. Moreover, all events related to remote connection protocols such as terminal protocols, industrial control protocols, and Internet control message protocol (ICMP), should also be logged. As mentioned above, at the first stage of an attack, adversaries usually perform reconnaissance of the system. Various remote connection protocols could be used for reconnaissance. Thus, network event logs will help security administrators to detect misbehaviour on the RAT server.

The generated logs should be stored securely in the log server. If the logs are stored in the system's local storage, there is a possibility that attackers can manipulate or harm the logs. Thus, event logs should be stored in a separate log server.

The log should be reviewed and analysed regularly by the security administrator.

8.5 Relationship between security threats and security controls

Table 1 shows the relationship between security threats and security controls, where an open circle in a cell indicates that a particular security control should be implemented to mitigate the specific threat.

Table 1 – Relationship between security threats and security controls

		7.1 Clients						7.2 Servers		7.3 Networks	
		T1	**T2**	**T3**	**T4**	**T5**	**T6**	**T7**	**T8**	**T9**	**T10**
Clients	8.1.1 Software update	O									
	8.1.2 Software integrity	O	O								
	8.1.3 Secure configuration	O	O	O							
	8.1.4 Control of user access				O		O				
	8.1.5 Physical security						O				
Servers	8.2.1 User authentication								O		
	8.2.2 User authorization						O				
	8.2.3 Periodic re-authentication						O				
	8.2.4 Software update							O			
Networks	8.3.1 Network access control									O	
	8.3.2 Mutual authentication								O	O	
	8.3.3 Misbehaviour detection					O				O	O
	8.3.4 Secure network configuration										O
Audits	8.4.1 Logging					O					

Appendix I

An example of a secure configuration of remote access tools in a sustainable energy resource

(This appendix does not form an integral part of this Recommendation.)

I.1 System overview

Many sensors and actuators are installed at generators. Sensors provide measured data to control devices (e.g., PLC in Figure I.1), and operators monitor the status of generators based on the data by using a HMI or engineering workstation. According to the status, operators control actuators via the HMI (or engineering workstation) and PLC. For example, when a typhoon comes, operators will stop the rotation of a wind turbine's blades. The network connecting sensors, actuators and control devices are called a *field network*. In the field network, a HMI for monitoring and controlling generators is usually installed.

Generators using sustainable energy resources, such as wind (wind turbines), hydrogen (fuel cells), and solar (photovoltaics), are operated by remote operators in some circumstances. Remote operators monitor the status of the generators and control them for efficiently generating electricity.

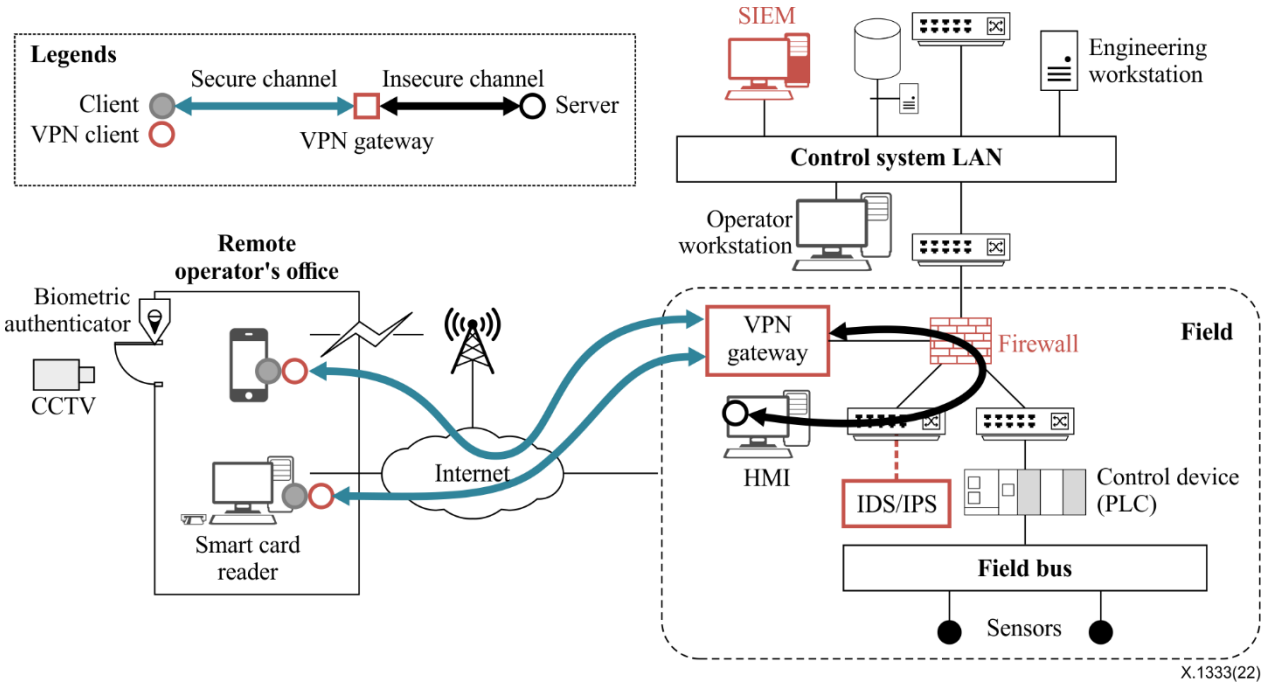

Figure I.1 – An example of a secure network for a sustainable energy resource control system

I.2 Secure configuration

Figure I.1 shows an example of a secure network configuration for a sustainable energy resource. In the remaining parts of this clause, security measures for each component, which includes the RAT client, RAT server, network and security event log, will be described.

I.2.1 RAT client

A separated account for the RAT client is created and the client software is accessed by the account only.

Whenever a remote operator turns on the RAT client software, the update check and integrity check processes are initiated, and the update will be applied before starting the RAT client software.

The NAC client checks the device's security level, and it blocks the Internet connection if any security configuration is missed. For example, anti-virus software and a personal firewall are not turned on, no communication connection is allowed by the NAC.

All devices running the RAT client are operated in the office of remote operators. Access control for the office is implemented using a biometric authenticator (e.g., fingerprint or facial recognition) and CCTV installed in front of the office door.

I.2.2 RAT server

When remote operators try to establish a RAT connection via a RAT client, two-factor authentication (i.e., password and smart card) is required. In addition, static IP addresses for a VPN gateway and RAT server are used.

Before mutual authentication, the host requesting a connection is filtered out by its IP address and media access control (MAC) address at the VPN gateway. Additionally, the lifetime of a communication channel between a VPN client and the VPN gateway is 8 hours. Thus, the remote operators must provide their password and smart card again for the VPN connection every 8 hours.

Accounts in the HMI for remote operators are separated from the other accounts to limit the permission of the remote operators and generate granular logs for the accounts.

I.2.3 Network

IPsec VPN protects a communication channel between a RAT client and server. Before connecting to the RAT server, a VPN client installed in a remote operator's device should establish a secure channel with a VPN gateway. To provide the 128-bit minimum level of security, the cryptographic suite, *Suite-B-GCM-256*, for IPsec VPN is used as in [b-IETF RFC 6379]. For IKEv2 authentication, *ECDSA-256* is applied for IPsec VPN as in [b-IETF RFC 6380]. For balancing security and overhead, the lifetime for IKE SA is set to 24 hours and the lifetime for IPsec SA is set to 8 hours.

The network for the field is divided into two segments, such as a DMZ for a HMI and a field network for PLCs, sensors and actuators. In addition, a firewall is located among the control system local area network (LAN), field network, and the DMZ for network segregation. Thus, a communication from an EWS on the HMI is allowed to transfer to the field network, but the firewall blocks any other traffic from the HMI to any other network.

An intrusion detection system (IDS) or IPS is installed in the DMZ and it receives incoming and outgoing network traffic from a switch port configured for traffic mirroring.

I.2.4 Security event log

Security events generated by remote access accounts are logged in the HMI system and they are transmitted to the security information and event management (SIEM) system. The security administrator of the organization operating the sustainable energy resource will review the logs periodically by using the SIEM system.

Bibliography

[b-ITU-T X.1197] Recommendation ITU-T X.1197 (2012), *Guidelines on criteria for selecting cryptographic algorithms for IPTV service and content protection.*

[b-IEC 61924-2] IEC 61924-2:2012, *Maritime navigation and radiocommunication equipment and systems - Integrated navigation systems – Part 2: Modular structure for INS - Operational and performance requirements, methods of testing and required test results.*

[b-IETF RFC 6379] IETF RFC 6379 (2011), *Suite B Cryptographic Suites for IPsec*.

[b-IETF RFC 6380] IETF RFC 6380 (2011), *Suite B Profile for Internet Protocol Security (IPsec).*

[b-Kruglov et al.] Kirill Kruglov, Evgeny Goncharov (2018), *Threats posed by using RATs in ICS*, Technical Report, Kaspersky Lab ICS CERT.
https://ics-cert.kaspersky.com/reports/2018/09/20/threats-posed-by-using-rats-in-ics/

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling, and associated measurements and tests
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	**Data networks, open system communications and security**
Series Y	Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2022